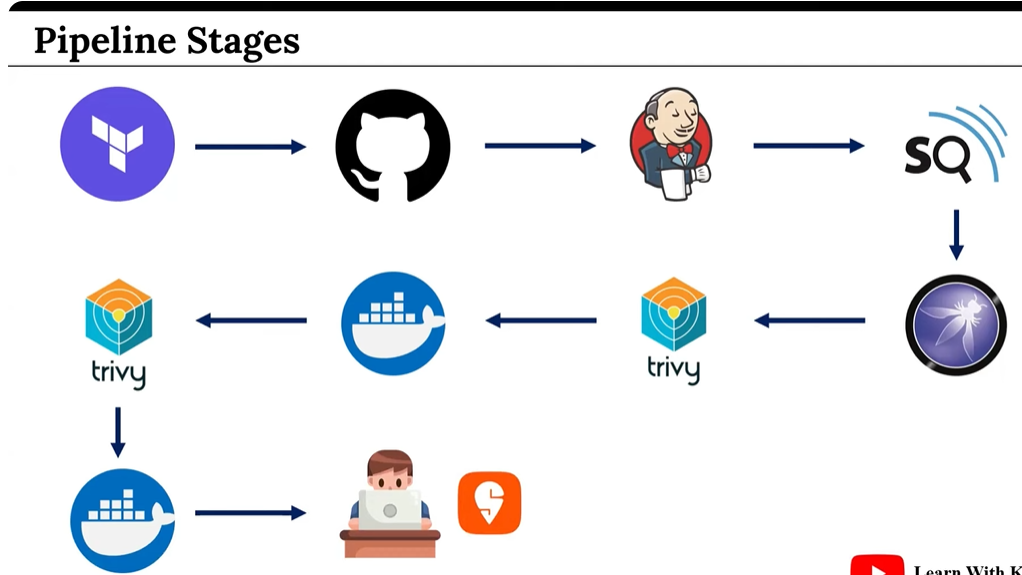
**Deployment of Swiggy App**

**==========================**

[**DevOps Real-time Project | Deployment of SWIGGY App | Kastro Kiran V**](https://www.youtube.com/watch?v=x55z7rk0NAU)

****

**git clone** [**https://github.com/juhisinha422/Terraform-Script-Swiggy.git**](https://github.com/juhisinha422/Terraform-Script-Swiggy.git)

* **Go to AWS -> IAM -> Create user: Swiggy -> Attach policies (administrator access) -> create user**
* **Create access key and secret key for above user.**
* **Initialize the terraform directory.**

**terraform init**

**terraform plan**

**terraform validate**

**terraform apply --auto-approve**

* **In EC2, we can see Swiggy Instance got created.**
* **Connect to Swiggy Instance using key.pem and mobaxterm or putty.**
* **Execute below commands.**

**$ sudo su**

**$ sudo apt update**

**$ java --version**

**$ sudo systemctl status jenkins**

* **Access the jenkins server now.**

**SwiggyPublicIP:8080**

* **Get jenkins password (from swiggy instance)**

**sudo cat /var/lib/jenkins/secrets/initialAdminPassword**

* **Connect to SonarQube now.**

**SwiggyIP:9000**

* **Login and change password.**
* **Similarly for Jenkins, create user and login.**
* **Go to Manage jenkins -> Plugins -> Available Plugins**
* **Install below plugins**
* [**Eclipse Temurin installerVersion**](https://plugins.jenkins.io/adoptopenjdk)
* [**Pipeline: Stage View**](https://plugins.jenkins.io/pipeline-stage-view)
* [**SonarQube Scanner**](https://plugins.jenkins.io/sonar)
* [**NodeJS**](https://plugins.jenkins.io/nodejs)
* [**OWASP Dependency-CheckVersion**](https://plugins.jenkins.io/dependency-check-jenkins-plugin)
* **Docker**
* **Docker Commons**
* **Docker API**
* **docker-build-step**
* **Go to Manage Jenkins -> Tools -> JDK Installations -> Add JDK -> name: jdk17 -> Install automatically -> Install from adoptium.net -> version: jdk-17.0.11+9**
* **Git install automatically**
* **SonarQube Scanner Installations -> Add SonarQube -> name: sonar-scanner -> Install automatically**
* **NodeJS Installations -> Add NodeJS -> name: node23 -> Install automatically**
* **Docker Installations -> add docker -> name: docker -> Install automatically -> download from docker.com -> version: latest**
* **Dependency-Check installations -> add dependency check -> name: DP-Check -> Install automatically -> Install from github.com**
* **Apply and Save.**
* **Integrate sonarqube with jenkins**
* **Go to Sonar -> Administration -> Security -> Users -> Token -> Name: token -> Generate -> copy**
* **Go to Manage Jenkins -> Credentials -> global -> add credentials -> kind: secret text -> Paste in secret (token) -> ID & Desc: Sonar-token -> Create**
* **Create sonarqube webhook -> Go to SonarQube -> Administration -> Configuration -> Webhooks -> create -> name: jenkins -> URL:** [**http://43.204.30.33:8080/sonarqube-webhook**](http://43.204.30.33:8080/sonarqube-webhook) **(Jenkins URL) -> create**
* **Configure sonarqube URL into jenkins**
* **Go to manage jenkins -> System -> SonarQube Servers -> Add SonarQube -> name: sonar-server -> Server URL:** [**http://43.204.30.33:9000**](http://43.204.30.33:9000) **-> Sonar authentication token : sonar-token-> save and apply**
* **Configure docker hub credentials into jenkins**
* **Go to manage jenkins -> Credentials -> global -> Add credentials -> kind: Username with password -> enter docker hub username and password -> ID & desc: docker-creds -> save**
* **Create jenkins job**
* **Go to dashboard -> New Item -> name: Swiggy App -> Select Pipeline -> OK -> Pipeline -> Paste script below**

**pipeline{**

**agent any**

**tools{**

**jdk 'jdk17'**

**nodejs 'node23'**

**}**

**environment {**

**SCANNER\_HOME=tool 'sonar-scanner'**

**}**

**stages {**

**stage('clean workspace'){**

**steps{**

**cleanWs()**

**}**

**}**

**stage('Checkout from Git'){**

**steps{**

**git 'https://github.com/KastroVKiran/DevOps-Project-Swiggy.git'**

**}**

**}**

**stage("Sonarqube Analysis "){**

**steps{**

**withSonarQubeEnv('sonar-server') {**

**sh ''' $SCANNER\_HOME/bin/sonar-scanner -Dsonar.projectName=Swiggy \**

**-Dsonar.projectKey=Swiggy '''**

**}**

**}**

**}**

**stage("quality gate"){**

**steps {**

**script {**

**waitForQualityGate abortPipeline: false, credentialsId: 'Sonar-token'**

**}**

**}**

**}**

**stage('Install Dependencies') {**

**steps {**

**sh "npm install"**

**}**

**}**

**stage('OWASP FS SCAN') {**

**steps {**

**dependencyCheck additionalArguments: '--scan ./ --disableYarnAudit --disableNodeAudit', odcInstallation: 'DP-Check'**

**dependencyCheckPublisher pattern: '\*\*/dependency-check-report.xml'**

**}**

**}**

**stage('TRIVY FS SCAN') {**

**steps {**

**sh "trivy fs . > trivyfs.txt"**

**}**

**}**

**stage("Docker Build & Push"){**

**steps{**

**script{**

**withDockerRegistry(credentialsId: 'docker-creds', toolName: 'docker'){**

**sh "docker build -t swiggy ."**

**sh "docker tag swiggy juhisinha/swiggy:latest "**

**sh "docker push juhisinha/swiggy:latest "**

**}**

**}**

**}**

**}**

**stage("TRIVY"){**

**steps{**

**sh "trivy image juhisinha/swiggy:latest > trivy.txt"**

**}**

**}**

**stage('Deploy to container'){**

**steps{**

**sh 'docker run -d --name swiggy -p 3000:3000 juhisinha/swiggy:latest'**

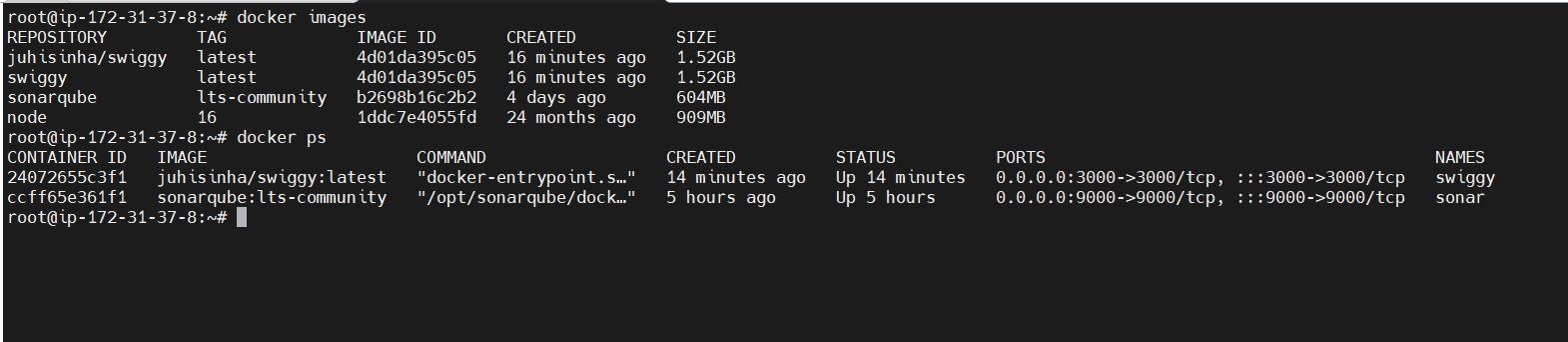
**}**

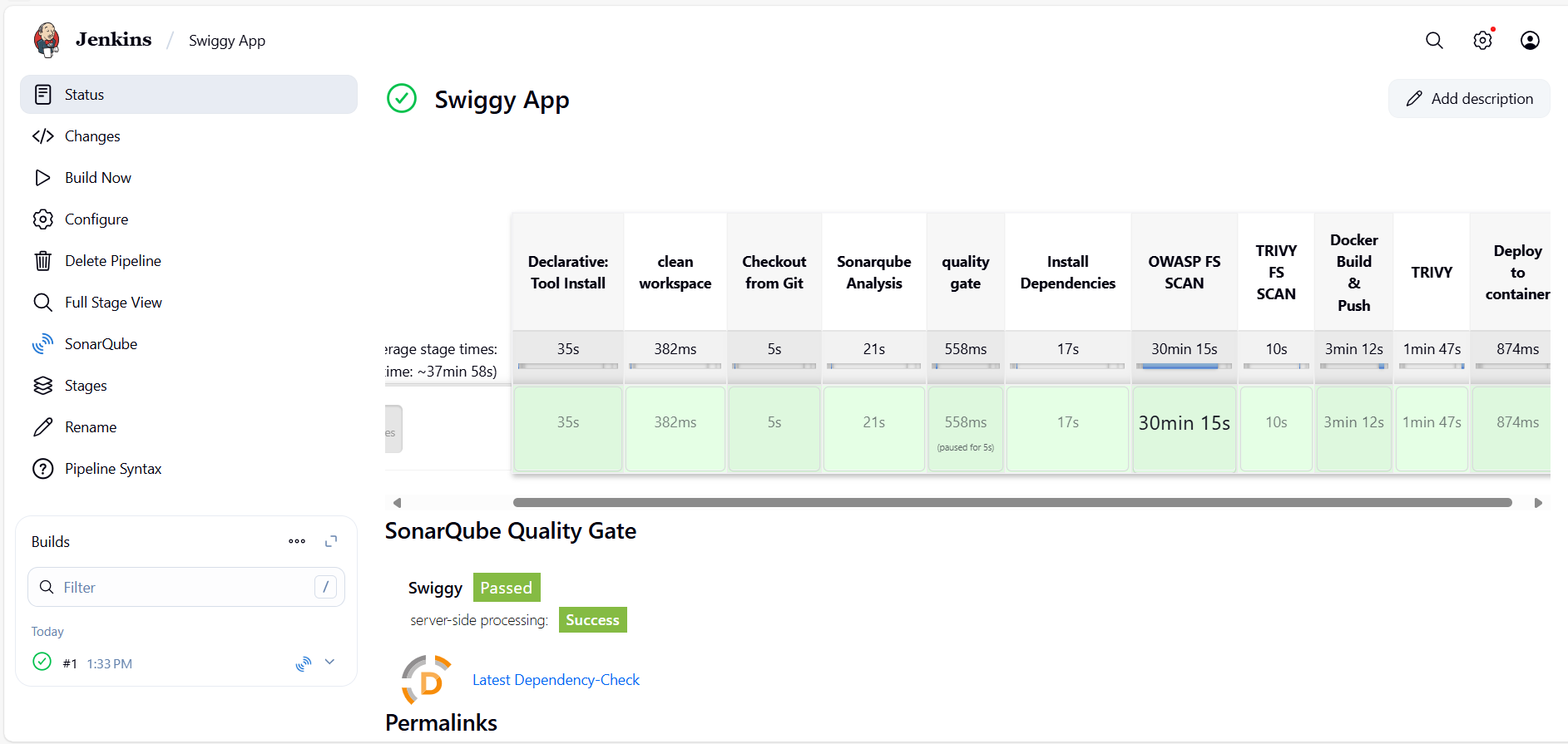
**}**

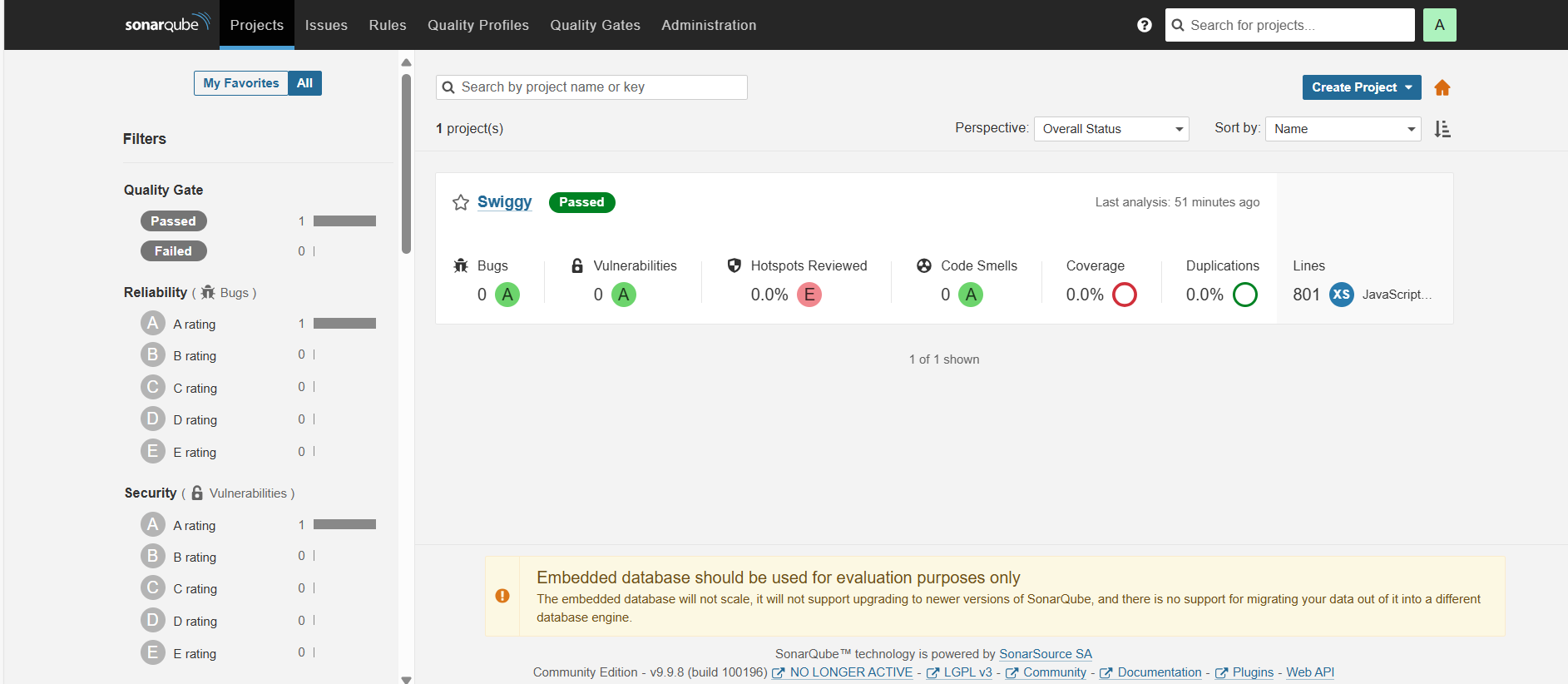
**}**

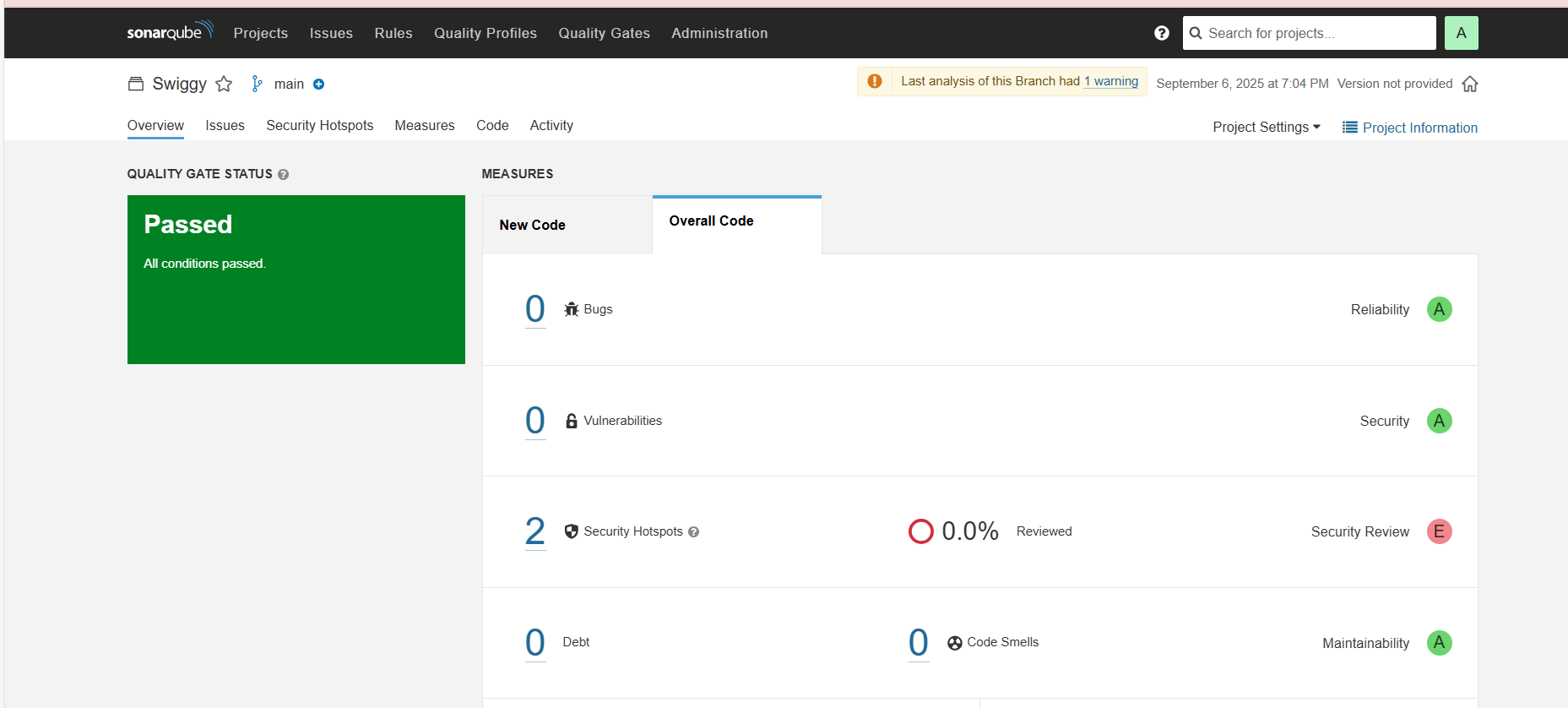
**}**

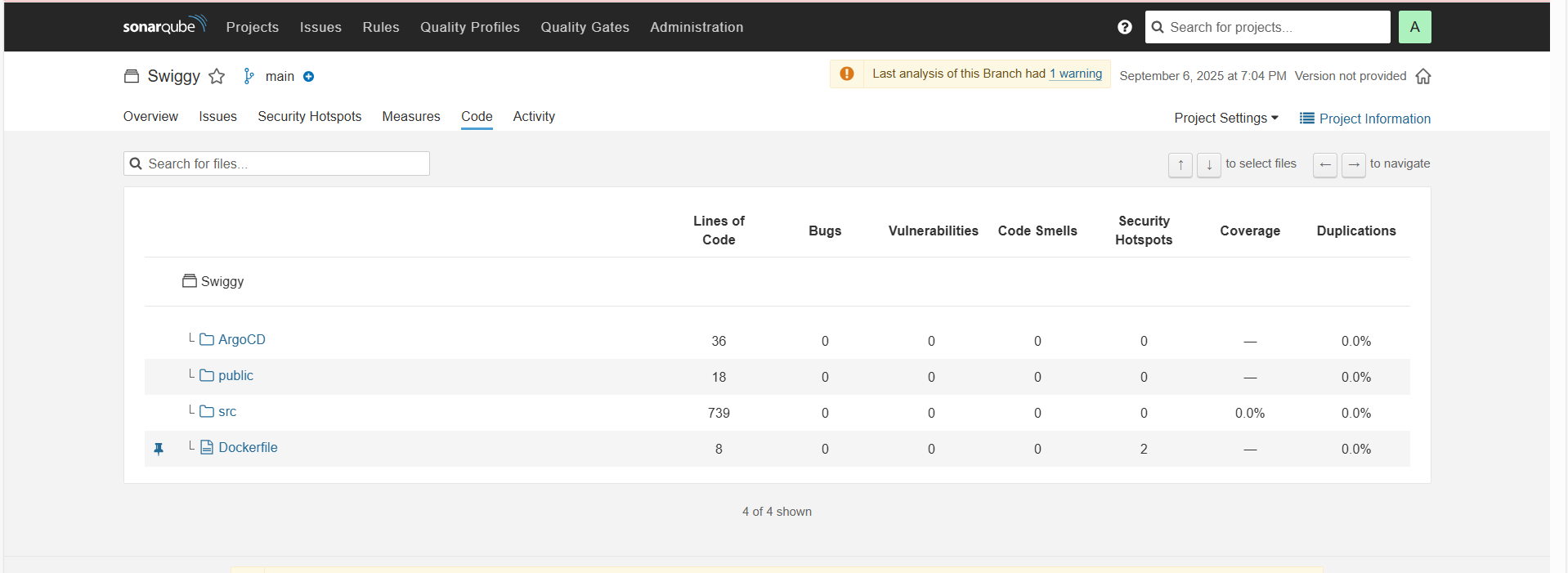
* **Apply, save and build now.**
* **Access the swiggy app: SwiggyPublicIP:3000/**

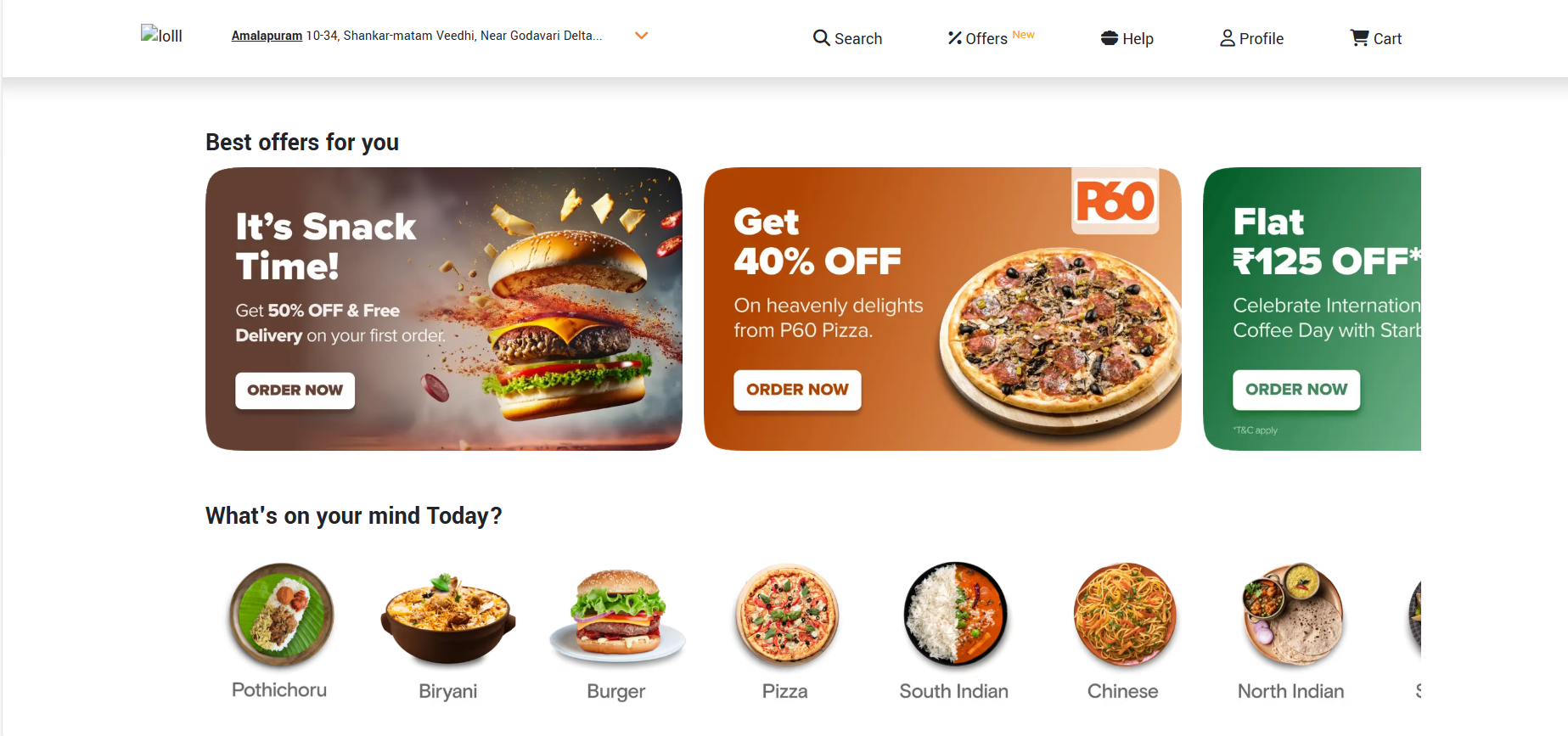
****

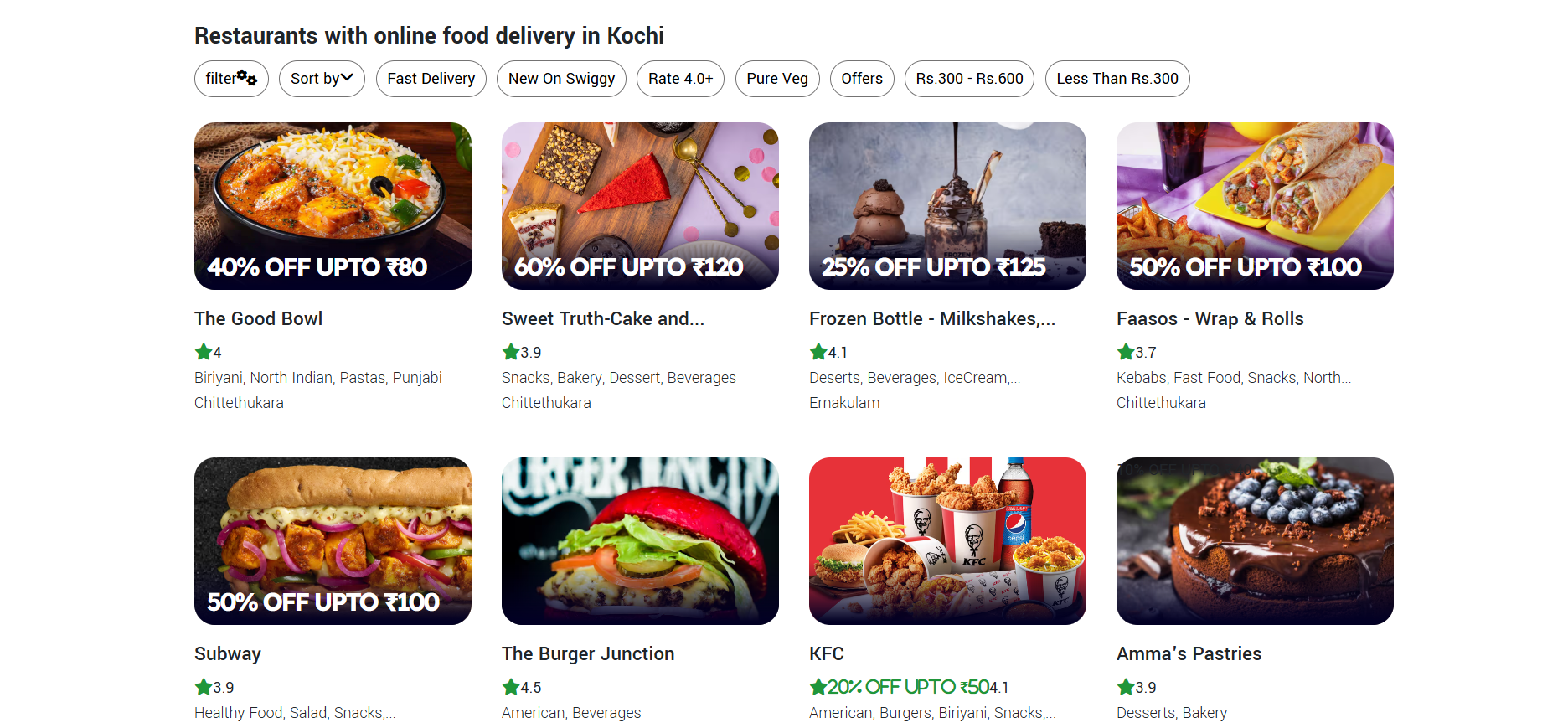
****

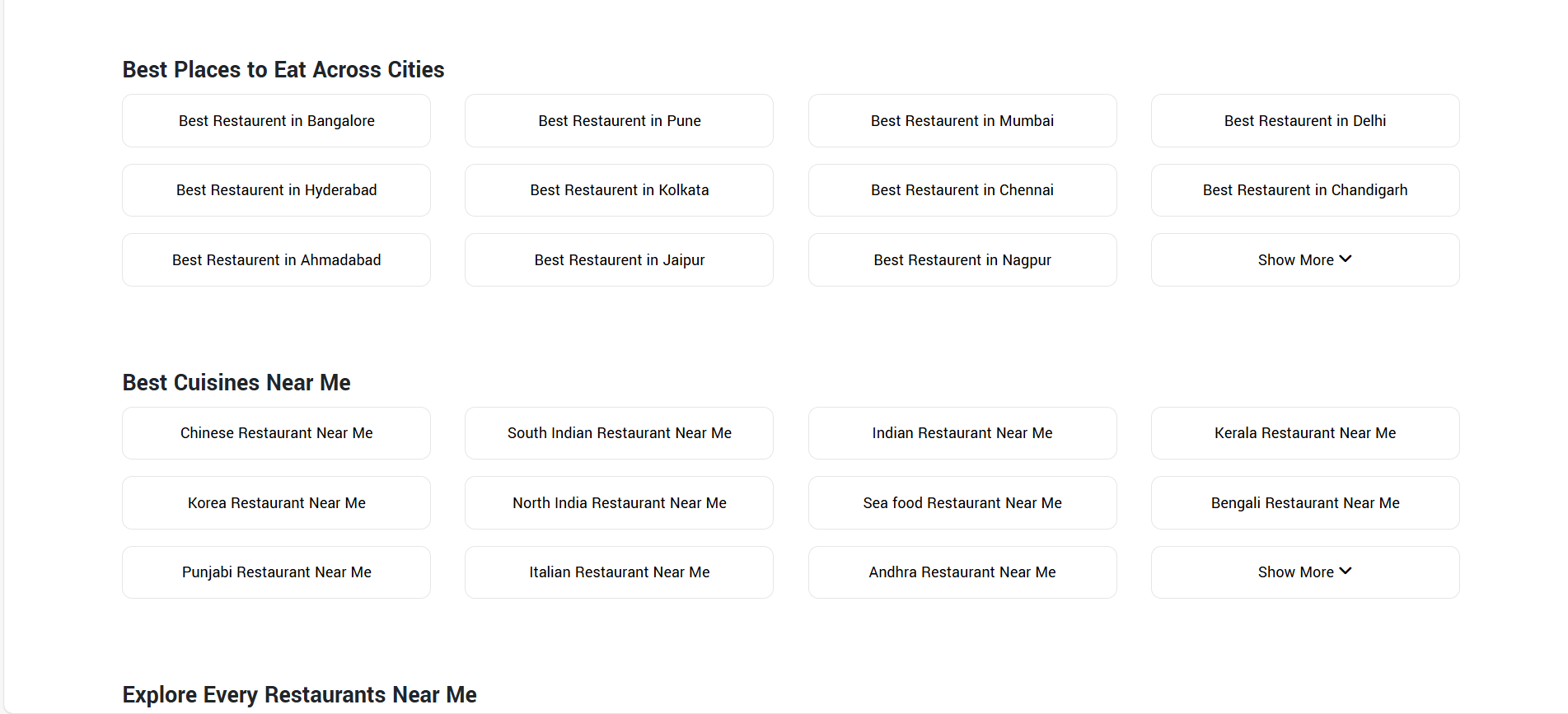
****

****

****

****

****

****